Noah J. Hanft
Senior Vice President
U.S. Region Counsel &
Assistant General Counsel

MasterCard International
Legal
2000 Purchase Street
Purchase, NY 10577-2509

914 249-5595
Fax 914 249-4261
E-mail noah_hanft@mastercard.com
Internet Home Page:
http://www.mastercard.com

4/27/1

(12)

MasterCard International

Via Hand Delivery

August 25, 2000

Communications Division
Office of the Comptroller of the Currency
250 E Street, SW, Third Floor
Washington, DC 20219
Attention: Docket No. 00-13

Ms. Jennifer J. Johnson
Secretary
Board of Governors of the Federal Reserve System
20th and C Streets, NW
Washington, DC 20551
Attention: Docket No. R-1073

2000 AUG 28 A 8:50

Robert E. Feldman
Executive Secretary
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429
Attention: Comments/OES

Manager, Dissemination Branch
Information Management & Services Division
Office of Thrift Supervision
1700 G Street, NW
Washington, DC 20552

Re: Proposed Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness

Ladies and Gentlemen:

This comment letter is filed on behalf of MasterCard International Incorporated ("MasterCard")[1] in response to the proposed Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness ("Proposal") published by the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision (collectively, the "Agencies").

MasterCard commends the Agencies for the general approach to information safeguards embodied in the Proposal. In particular, we applaud the Agencies for proposing an approach which recognizes the importance of providing flexibility to each financial institution to structure its safeguards "commensurate with . . . the complexity and scope of the [financial institution] and its activities." This is a critically important aspect of the Proposal which will allow each financial institution to design safeguards that are best suited to the operations and activities of that financial institution. We offer the following more specific comments for consideration by the Agencies when adopting the Proposal in final form ("Final Standards").

In General

The Agencies have issued the Proposal in response to section 501 of Title V of the Gramm-Leach-Bliley Act (the "GLB Act") which directs the Agencies to establish appropriate standards for use by financial institutions in safeguarding "customer records and information." The Supplementary Information to the Proposal states that "[w]hile this [P]roposal is in the form of guidelines, the Agencies solicit comment on whether the [F]inal [S]tandards should be issued in the form of guidelines or as regulations." We applaud the Agencies for issuing the Proposal in the form of guidelines, and we urge that the Final Standards be issued in the same form. Based on our experience, we believe that it is important that the standards used for safeguarding sensitive information be flexible enough to allow for the rapid modifications needed to address new threats as they develop. To ensure that the Final Standards establish the necessary level of flexibility, it is important that the standards be issued as guidelines which give general direction to financial institutions while enabling each financial institution to develop policies and procedures best suited to its own operations and experiences. If the Final Standards are issued as regulations, they will be more rigid than would be appropriate in light of the

[1] MasterCard is a membership organization comprised of financial institutions which are licensed to use the MasterCard service marks in connection with payment systems, including credit cards, debit cards, smart cards and stored-value cards.

speed with which financial institutions must be able to respond to technological and other changes in the dynamic environment surrounding information practices.

We also note that the Supplementary Information indicates that "[k]ey components of the [Proposal] were derived from security-related supervisory guidance previously issued by the Agencies and the Federal Financial Institutions Examination Council (FFIEC)." We applaud the Agencies for using existing security-related guidance as the basis for important parts of the Proposal. In our view, the supervisory guidance previously issued by the Agencies and FFIEC effectively addresses many of the issues covered by the Proposal. In addition, using existing security-related supervisory guidance as the basis for key elements of the Final Standards would be a highly efficient approach since most financial institutions already have programs in place to comply with that guidance. Accordingly, we urge the Agencies to retain this approach in the Final Standards. Moreover, we urge that the Agencies make it clear in the Final Standards that a financial institution's compliance with existing supervisory guidance on security-related issues will constitute compliance with applicable portions of the Final Standards themselves. This clarification is important to avoid any implication that the Agencies are imposing additional or different standards in those instances where the Agencies simply intend to incorporate existing guidance in the Final Standards.

Scope

The Proposal makes clear that it applies only to "customer information maintained by or on behalf of a financial institution." In the Supplementary Information, the Agencies recognize that by limiting the Proposal to "customer information" it will not apply to "consumers" who have not established an ongoing relationship with a financial institution or to "business" customers of a financial institution (i.e., customers who obtain financial products or services for a business purpose rather than for personal, family, or household purposes). This is an important distinction that should be retained in the Final Standards. The Supplementary Information, however, indicates that the Agencies have considered expanding the scope of the Proposal to cover, among other things, records regarding all *consumers* of a financial institution. We believe that any such expansion of the Proposal would be inconsistent with the plain language of the GLB Act.

Section 501 of the GLB Act directs the Agencies to establish standards for safeguarding records and information relating to "customers" rather than "consumers." The Agencies recognized the significance of this distinction in connection with the recently issued regulations implementing the other privacy provisions of the GLB Act ("Privacy Rule"). Specifically, in a discussion titled "Distinction Between 'Consumer' and 'Customer'," the Supplementary Information to the Privacy Rule states that "[t]he Agencies believe . . . that the distinction [between 'consumer' and 'customer'] was deliberate and that the [Privacy] [R]ule should implement it accordingly." 65 Fed. Reg. 35162, 35166 (June 1, 2000). The Supplementary Information explains that "[a] plain

reading of the [GLB Act] supports the conclusion that Congress created one set of protections . . . for anyone who obtains a financial product or service [(*i.e.*, "consumers")] and an additional set of protections . . . for anyone who establishes a relationship of a more lasting nature than an isolated transaction with the financial institution [(*i.e.*, "customers")]." *Id.* Congress made the same distinction when enacting section 501 of the GLB Act and limited that section to "customer" information. We applaud the Agencies for honoring this distinction in the Proposal, and we urge that the distinction be retained in the Final Standards.

We also commend the Agencies for limiting the Proposal to information regarding customers who obtain financial products or services from a financial institution for "personal, family, or household purposes." As the Agencies acknowledged in the Privacy Rule, the privacy provisions included in the GLB Act apply "only to nonpublic personal information about individuals who obtain financial products or services primarily for personal, family, or household purposes [and do] not apply to information about companies or about individuals who obtain financial products or services for business, commercial, or agricultural purposes." *Id.* at 35196. We urge the Agencies to continue to use this same approach by ensuring that the Final Standards apply only to "customers" who obtain financial products or services for "personal, family, or household purposes." We acknowledge, however, that financial institutions may choose to utilize the guidance provided in the Final Standards for developing security safeguards applicable to "consumers," business clients, and other entities not covered under section 501 or the Proposal. However, the GLB Act does not, and the Final Standards should not, *require* them to do so.

Definitions

Definition of Customer and Customer Information

Under the Proposal, the term "customer" would be defined by using the same definition set forth in the Privacy Rule. In addition, the Proposal defines "customer information" as any information containing "nonpublic personal information" (as defined in the Privacy Rule) "about a customer, whether in paper, electronic or other form . . . maintained by or on behalf of" a financial institution.

We commend the Agencies for proposing these definitions, and we urge that they be retained in the Final Standards. In particular, it is important that the definitions of "customer" and "customer information" be consistent with corresponding definitions set forth in the Privacy Rule. Financial institutions will be able to protect "customer" privacy most effectively only if they can readily determine which information is subject to both sets of requirements. Any suggestion that the term "customer" or "customer information" would have different meanings under the Final Standards and the Privacy Rule would create confusion and make it more difficult for the personnel who have

primary responsibility for implementing the two rules to do so. Moreover, there is nothing in the GLB Act or its legislative history that would even suggest that the terms "customer" or "customer information" should have different meanings under the Final Standards than they do under corresponding provisions of the Privacy Rule. Accordingly, we believe that the Agencies have chosen the most appropriate definitions for "customer" and "customer information," and we urge that they be retained in the Final Standards.

Definition of Service Provider

Under the Proposal, the term "service provider" would be defined as "any person or entity that maintains or processes customer information on behalf of the [financial institution], or is otherwise granted access to customer information through its provision of services to the [financial institution]." This definition appears to be focused on entities that provide administrative and other similar services to financial institutions. We are concerned, however, that the definition could be interpreted broadly to cover attorneys who obtain information from financial institutions in connection with providing legal services, or accountants and other similar professionals who obtain information for auditing or similar purposes. Covering such communications would appear to be unnecessary in view of the strong ethical duties that attorneys and accountants must adhere to with respect to information they receive from their clients. Moreover, imposing any restrictions under the GLB Act on communications between financial institutions and their attorneys and accountants could be counterproductive in many instances, particularly when a financial institution needs to urgently retain counsel or the services of an accountant. Accordingly, we urge that the definition of "service provider" be modified to clarify that it would not cover attorneys, accountants, or other similar professionals.

Standards for Safeguarding Customer Information

The Proposal states that "[e]ach [financial institution] shall implement a comprehensive information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the [financial institution] and the nature and scope of its activities." We applaud the Agencies for acknowledging that each financial institution has the flexibility to design its own information security program based on its size, complexity, and other factors. We urge that this flexibility be retained in the Final Standards. We request, however, that the Final Standards provide further clarification regarding how to structure the financial institution's "comprehensive information security program." In particular, we are concerned that the requirement for a "comprehensive" information security program could be construed to require that a financial institution establish a single program applicable to all of the business lines and all of the entities included within the financial institution's corporate family. Such an interpretation could be extremely difficult to implement for many financial institutions that have a wide variety of business lines with different customer bases, and varying levels of technological, staffing, and other resources. Indeed, this requirement may run counter to

the Agencies' desire to establish safeguards "commensurate with . . . the complexity and scope of the [financial institution] and its activities." In order to address this issue, we urge that the Agencies make it clear that although a financial institution's security program must be "comprehensive" in that it covers all customer information of the financial institution, the financial institution need not use the same security program for all of its business lines or affiliated entities.

The Proposal also states that one of the objectives of a financial institution in establishing a security program shall be to "[e]nsure the security and confidentiality of customer information." This language appears to be intended to implement section 501(b)(1) of the GLB Act which directs the Agencies to establish appropriate standards for financial institutions "to insure the security and confidentiality of customer records and information." We are concerned, however, that use of the word "ensure" suggests that the Agencies intend to establish a standard which would be impossible to satisfy. In this regard, no security program is perfect and it simply is impossible to "ensure" perfect compliance in all cases. In order to address this issue, we request that the Agencies use the word "protect" rather than "ensure." This would be consistent with the Agencies' articulation of the other objectives for safeguarding customer information and would provide appropriate guidance to financial institutions without establishing a standard which is impossible to meet.

In the Supplementary Information, the Agencies have clarified that while financial institutions are to protect against unauthorized access to customer information, "unauthorized access" does not include access to or use of information with the customer's consent. This is a helpful and important clarification which should be included in the text of the Final Standards themselves.

Development and Implementation of Information Security Program

The Proposal describes the level of involvement that the board of directors and management of a financial institution should have in developing and implementing an information security program. With respect to involvement of the board of directors, the Proposal states that the board must:

> a. Approve the financial institution's written information security policy and program that complies with the Final Standards; and
>
> b. Oversee efforts to develop, implement, and maintain an effective information security program.

We acknowledge that appropriate participation by a financial institution's board of directors is an important part of establishing an effective information security program. We are concerned, however, that the Proposal could be interpreted as requiring a financial

institution's board of directors to become involved in developing and implementing information security programs at a level of detail which simply is not appropriate or feasible for many boards. For example, the Proposal would require a board of directors to approve written information security programs which in many instances would be extremely lengthy and would set forth detailed technological, legal and other specifications. In order to avoid the inference that a board must review or approve programs at a detailed level, we urge that the Proposal be modified to make it clear that a financial institution's board of directors has the responsibility for guiding the financial institution's strategic direction by approving policies that establish principles and goals for use by the institution's management in developing information security programs. The Final Standards should also make it clear that it is management's responsibility (and not the board of directors') to develop, approve, and implement the details of the information security programs.

The Agencies have specifically invited comment whether the Final Standards should specify how frequently management must report to its board of directors regarding a financial institution's information security program (*e.g.*, monthly, quarterly, annually). We urge the Agencies to refrain from requiring any specific time interval for reporting to boards of directors on information security issues. In our view, this matter should be decided by each financial institution based on its own corporate governance principles which guide interaction between management and its board of directors. Should the Agencies decide to include a specific time interval, we would urge that reporting be required no more often than annually.

The Agencies also have requested comment on whether the Final Standards should require the board of directors to designate a "Corporate Information Security Officer" or other responsible individual who would have the authority (subject to the board's approval) to develop and administer the institution's security program. We believe that financial institutions should retain the flexibility to determine how best to staff and manage information security issues, and we urge the Agencies to refrain from requiring financial institutions to designate a particular individual for this purpose.

Manage and Control Risk

The Proposal provides guidance on the elements that a financial institution "should consider" in establishing policies and procedures to manage and control information security risk. Specifically, the Proposal states that each financial institution should consider appropriate: (a) access rights to customer information; (b) access controls on customer information systems, including controls to grant access only to authorized individuals and companies; (c) access restrictions at locations containing customer information; (d) encryption of electronic customer information; (e) procedures to confirm that customer information system modifications are consistent with the financial institution's information security programs; (f) dual control procedures, segregation of

duties, and employee background checks for those with access to customer information; (g) contract provisions and oversight mechanisms to protect the security of information maintained by service providers; (h) monitoring systems and procedures to detect attacks on or intrusions into customer information systems; (i) programs that specify responses to be taken when unauthorized access is suspected or detected; (j) protection against destruction of customer information; and (k) response programs to preserve the integrity and security of customer information in the event of computer or other technological failure.

We applaud the Agencies for providing general guidance that financial institutions "should consider" in designing policies and procedures to control information security risks. We believe that a number of additional clarifications would be helpful, however, and we offer the following specific suggestions. First, we urge that the Supplementary Information to the Final Standards state that the enumerated factors are examples and not mandatory components of a financial institution's information security program. A financial institution should not be required to adopt policies and procedures that address every one of the factors the Agencies have enumerated for consideration. In this regard, the Final Standards should make it clear that each financial institution has the ultimate discretion to determine the policies and procedures most appropriate for its information operations, provided that the policies and procedures satisfy the objectives specified in the Proposal.

Second, we urge that the Final Standards clarify the Proposal's reference to "access rights" to customer information. In particular, we urge that the Final Standards make it clear that they do not require a financial institution to allow consumers to access information the financial institution maintains on those consumers. Although such information access rights have been considered as part of a number of legislative and other proposals, such rights were not included in the GLB Act and should not be created as part of the Final Standards.

Third, we urge that the reference to "encryption" be eliminated as a separate factor a financial institution should consider in establishing policies and procedures to control information security risk. We are concerned that by listing encryption as a separate factor a financial institution must consider, the Agencies may raise the inference that encryption techniques must be used more widely than would be appropriate or cost effective. For example, the Proposal's reference to encryption could be interpreted as advocating that encryption be used for virtually all customer information. Such broad use of encryption would be difficult to justify, particularly where other controls already are in place to prevent unauthorized or fraudulent access.

In addition to specifying factors a financial institution should consider in developing a security program, the Proposal would require a financial institution to "[t]rain staff to recognize, respond to, and where appropriate," report unauthorized or fraudulent

attempts to obtain customer information. We agree that training appropriate personnel is an important part of controlling information security risk. We urge, however, that this provision be modified to make it clear that a financial institution need not provide information security training to every employee of the financial institution. This clarification could be accomplished by stating in the Final Standards that such training requirements relate only to those employees who are in a position to recognize unauthorized or fraudulent attempts to gain access to customer information.

The Proposal also indicates that a financial institution must regularly test key controls, systems, and procedures of its information security program and that the tests "shall be conducted, where appropriate, by independent third parties or staff independent of those that develop or maintain the security programs." The Proposal also states that "[t]est results shall be reviewed by independent third parties or staff independent of those that conducted the test." Although we agree that systems should be tested to determine that they are working properly, we are concerned that the Proposal would mandate a cumbersome, multi-tiered process. Under the Proposal, there must be at least three layers of personnel involved in system testing — (i) personnel responsible for developing the system; (ii) personnel responsible for conducting the test; and (iii) personnel responsible for reviewing test results. Such an approach would be difficult for many financial institutions (particularly smaller institutions) to implement. Also, it appears difficult to justify requiring special test procedures for information security when financial institutions routinely use more well established approaches, such as internal and external audits to test compliance regarding the many other legal requirements imposed on regulated financial institutions. In order to address this issue, we urge that the Final Standards refrain from establishing special test procedures and instead simply indicate that management may rely on internal audit, external audit, or other qualified professional sources to conduct tests of its key information security features.

The Agencies have requested comment on whether specific types of security tests, such as penetration tests or intrusion detections tests, should be required. We urge the Agencies to refrain from imposing such a requirement. Information security testing is continually evolving. What may appear appropriate or effective now may not be the most effective test in the near future. Therefore, to require specific tests may actually stunt the development of a financial institution's procedures for evaluating its security program. It should be sufficient to require each financial institution to perform its own testing and to clarify that the burden is on the financial institution to establish testing procedures best suited to its own operations.

Oversee Outsourcing Arrangements

Under the Proposal, a financial institution would continue to be responsible for safeguarding customer information, even when it is in the hands of a third party service provider. Specifically, the financial institution would be required to exercise "appropriate

due diligence" with respect to its outsourcing arrangements to confirm that service providers have an "effective information security program" and customer information systems consistent with the Proposal.

We understand the importance of maintaining the security of information given to third party service providers. We are concerned, however, with the approach taken by the Agencies. The Proposal suggests that financial institutions must actively *manage* and *monitor* the information security practices of third party service providers. Such a requirement would be extremely burdensome, especially for smaller financial institutions. To address this issue, we urge that the Final Standards acknowledge that, where appropriate, financial institutions may utilize more traditional means of restricting the information practices of service providers, such as by contractually imposing responsibility on service providers to employ proper information protections. Although these contractual provisions do not necessarily involve the financial institution actively monitoring or testing the service provider, they do allow the financial institution to take appropriate steps if weaknesses are detected.

We would also urge the Agencies to delete the requirement that financial institutions confirm that third party service providers have "implemented an effective information security program and customer information systems consistent with" the Proposal. While financial institutions need to consider a service provider's ability to guarantee the security of customer information, financial institutions cannot be expected to evaluate each service provider's security program in light of the Proposal.

Effective Date

The Proposal provides that a financial institution must be in full compliance with the Final Standards by July 1, 2001. We commend the Agencies for striving to provide adequate time for financial institutions to implement appropriate information security programs, and we urge that the Final Standards require compliance no earlier than July 1, 2001.

In addition, we urge the Agencies to consider extending the deadline for compliance based on the date on which the Final Standards are published. Specifically, we request that the Agencies consider providing to financial institutions a year after publication of the Final Standards in which to review their information security programs in light of the Final Standards. Although many financial institutions have information security standards that are generally consistent with the Proposal, adjustments may be necessary after the Final Standards are published. In view of the significance of these programs, it is important that financial institutions have adequate time to develop, implement, and test any changes or additions to their programs before the final effective date, and doing so by July 1, 2001 may be difficult in view of the considerable resources

that many financial institutions have been required to devote to implementing procedures to comply with the Privacy Rule by July 1, 2001.

* * * * *

Once again, MasterCard commends the Agencies for their efforts in drafting the Proposal, and we greatly appreciate the opportunity to provide our comments. If you have any questions concerning this comment letter, or if we may otherwise be of assistance in connection with this issue, please do not hesitate to call me, at the number indicated above, or Michael F. McEneney at Sidley & Austin, at (202) 736-8368, our counsel in connection with this matter.

Sincerely,

Noah J. Hanft

Noah J. Hanft

cc: Joshua Peirez (MasterCard International)
Michael F. McEneney (Sidley & Austin)